Follow-up Report
Corrective Action Plan (CAP): Audit Report #08DP-02
State Web Server Security Audit
Department of Administration (DOA)
February 27, 2009

Agency	Recommendation #	Does this affect a federal program?	CFDA # (if previous YES)	Management View	CAP – Corrective Action Plan	Person responsible for CAP	Target Date
61010 DOA	**<u>Recommendation #1</u>** We recommend the Department: **A**. Define state web server and web server application security responsibilities in policy. **B**. Notify all state agencies of their web server and web server applications security responsibilities. **C**. Implement procedures to comply with Enterprise Security policy ENT-SEC-012	No		Concur	**A.** The Department is publishing policies based on the National Institute of Standards and Technology (NIST) by working previously published guidelines into the security standards established by NIST. The Department will modify and selectively apply the NIST standards based on the best interests of the State of Montana. **B. and C:** Once the Information Systems Security Policies are in place, the Department will implement a security program for all state agencies to identify risks, threats and vulnerabilities so they are able to make decisions about the security of their information assets and supporting systems. Of the 18 statewide policies that are associated with this effort, two are complete and published and six are to be complete and published within the next 90 days. The remaining policies are to be complete by February 2010.	Dick Clark Dick Clark	2/1/10 Being Implemented 3/1/10 Being Implemented

Agency	Recommendation #	Does this affect a federal program?	CFDA # (if previous YES)	Management View	CAP – Corrective Action Plan	Person responsible for CAP	Target Date
61010 DOA	**<u>Recommendation #2</u>** We recommend the Department of Administration scan the De-Militarized Zone for rogue servers on a regular basis.	No		Concur	The department has implemented our Intrusion Detection System in the Helena De-Militarized Zone. This assists in monitoring for "rogue servers" in this area of the network. We will be implementing the system in the Billings De-Militarized Zone in a few weeks.	Dick Clark	9/1/09 Being Implemented
					The Network and Operations Security Center (NOSC), is working with the web group to monitor the web environment with the new Web Defend product for security related issues and will follow up on any unusual activity.	Dick Clark	3/1/09 Implemented